[0092] FIG. 4 displays the main components for a preferred embodiment of the single channel schema of the present invention. The user 401 would visit the server 407 of the present invention and the server 407 would provide applets 470 for downloading to the user's device 403 via path 420. The user 401 downloads an applet 470 via path 421 which is then stored on the device 403 as the customer applet 422. The web merchant 405 would also visit the Authorization Server 475 ~~407~~ via path 450 and download ~~the~~ an applet 470 via path 451 which is stored on the merchant site 405 as merchant applet 452. The user 401 using the device 403 visits the web merchant site 405 via path 430 and selects items they wish to purchase by placing them in the basket 406 and selecting the appropriate credit or debit card for use 407. The merchant site 405 then accumulates the items in the basket 406, information about the card 407, and utilizing the merchant applet 452 routes the information along path 431 to the Authorization Server 407.

Please amend Paragraph [0102] as follows:

[0102] FIG. 8 represents an additional schema utilizing features of the present invention in which a user has a pre-authorized or debit account 804. The user would see a live device 805, such as a vending machine, and would select items via path 820 ~~810~~ thereby triggering the live device 805 to demand payment via path 810. The payment demand would be routed through the preauthorized liquid account 804 which is done by swiping the pre-authorized account 804, such as a credit or debit card, in step 840 through a card swipe device 806. In addition the micro payment demand would also notify the card swipe device 806 that a TAC would be requested. The user may have a personal device 803, such as a wireless phone, which would contain either a TAC or security string whereby the user would determine the TAC and enter the TAC 830 into the card swipe device 806. Alternatively, the user could enter the TAC 830 into the wireless device 803 which would wirelessly transmit the TAC 830 to the card swipe device 806 or Authorization Server 807. The details of the transaction are sent along path 850 from the card swipe device 806 to the Authorization Server 807. The Authorization Server 807 contains the information on the liquid account and if verified would notify a micro payment host 808 along path 860 to authorize payment. The micro payment host 808 then transfers payment along path 870 to the live device 805.

Please amend Paragraph [0117] as follows:

[0117] The inputting of a Username, Password or PIN number in a computer, portable digital assistant ("PDA"), 2.5G or 3G mobile device is currently flawed for the following reasons: (1) the User can be seen from onlookers entering their PIN number into the device (called `shoulder surfing`); (2) the keyboard could contain a `Trojan` program that records the inputted Username, Password or PIN number (Trojans are downloaded without the knowledge of the User onto a computer and can reside there indefinitely); (3) PKI Certificates authenticate that the transaction was conducted on a certified computer, but they do not effectively authenticate the User behind the computer; and (4) computers running Microsoft Windows have a problem because Windows remembers the Username, Password or PIN number which creates a situation where the device stores the I/D of the User within the computer.

Please amend Paragraph [0121] as follows:

[0121] Further, the user interface is easy to use because the user need know nothing about the protocol, TAC's and Security Strings. The PIN Safe user would merely input their unchanging PIN via the Pin Safe user interface. Further, the Pin Safe user interface is "tempest" proof because the interface does not display the users PIN or TAC (Pseudo PIN) on screen, and therefore is not subject to Electro-magnetic emissions from the video display unit ("VDU") that could be the subject of surveillance via Tempest technologies. The strong protection gained by using the Pin Safe user interface of the present invention allows safe single PIN usage on a variety of accounts with differing security architectures which can be achieved by using a central PIN Authorization Server. Even if the security string resides on the device it is not a problem because the present invention does not require a digital certificate and therefore there is nothing in the memory of the computer that compromises the Users I/D if it falls into the wrong hands.

Please amend Paragraph [0130] as follows:

[0130] In addition, the Pin Safe or Radar Interface can work within a computers own processor, within a local area network ("LAN") configuration, and over the Internet. Operating within a computers own processor the Pin Safe interface could act as a hack proof screensaver which means that when a user first started their computer they will be presented with the interface. The user must input their PIN accordingly and if the user decided to leave the computer for a short time, where there is the opportunity for criminal use of his computer, the user could press a

function key which would activate the Pin Safe interface. Upon returning to the their computer they would simply click on their mouse or any key and enter their PIN via the Pin Safe interface.

Please amend Paragraph [0137] as follows:

[0137] As seen in FIG. 18, the Security String is sent from authorization computer 1807 to the User's mobile device 1804. The user 1801 inputs the TAC via the Pin Safe interface 1823 and the Authorization Server 1807 receives the TAC via the Internet 1813.

Please amend Paragraphs [0141] and [0142] as follows:

[0141] FIG. 21, shows a typical data access application where an Authorization Server 2107 has been fitted to a Gateway Server 2109 accessing a Database 2111, the Database 2111 being protected by a firewall 2115. FIG. 21 assumes that the user 2101 has registered with the system and has the Pin Safe Interface applet 2123 on their computer which allows the user 2101 to communicate with Authorization Server 2107 via the Internet 2113 using paths 2120, 2140, and 2152. To access information from the Database 2111 the Authorization Server 2107 sends a new security string to the user's computer or G2 mobile phone 2104 via the Internet 2113 or through a wireless connection 2151. The security string 2151 resides on the device 2104 until the user 2101 wishes to access the Database 2111.

[0142] The User 2101 sends his volatile TAC to the Authorization Server 2107 to confirm his/her identity. In the dual channel scenario the user obtains their TAC from the G2 mobile device 2104 via either visual extraction (using their PIN as a sequencer) or Smart PIN or standard inline memory module ("SIMM") extraction where the User 2101 enters their PIN into the device 2104 and the relevant TAC digits are displayed on the device 2104 screen. The TAC is then inputted into the user's computer (not shown). In the single channel scenario the user simply inputs their PIN into the Pin Safe interface 2123. The PIN is then converted into a TAC within the applet 2123 and transmitted via path 2120 to the Authorization Server 2107

Please amend Paragraph [0146] as follows:

[0146] FIG. 23 shows the Generic Integration Platform which displays the Authorization Server 2307 inside a firewall 2315 ~~2215.~~ The Authorization Server 2307 is connected to a Net Server 2317 and a host database 2311. The host database 2311 may also be inside it's own firewall 2316.

Please amend Paragraph [0148] as follows:

[0148] Any reference herein to a computer means any personal computer, ATM, PDA, G2.5 Mobile Device, G3 Mobile Device, or any device with a central processing unit ("CPU"). Any reference herein to a transaction means any financial transaction, remote Data Access procedure, or any interface transaction between a user and a system. The numbers on the various user interfaces and displays are merely exemplary and the use of characters, letters, colors and such may be used individually or in combination and still fall within the intended scope of the present invention.

Please amend the Abstract as follows:

A method and system for secure identification of a person in an electronic communications environment, wherein a host computer ~~is adapted to be able to~~ communicates with a plurality of user-operated electronic devices. ~~operated by the user. The user is issued with a user code, known only to the user and stored in the host computer.~~ When the user is required to identify themselves to the host computer, the host computer generates a pseudo-random security string and applies a previously issued ~~the~~ user code to the ~~pseudo-random~~ security string to generate a transaction code. The host computer also transmits the ~~pseudo-random~~ security string to one of the electronic devices for display ~~which is displayed by the electronic device~~ to the user. The user applies the ~~their known~~ user code to the displayed ~~pseudo-random~~ security string and determines the transaction code. The ~~user enters the~~ transaction code is entered into an electronic device ~~and the entered transaction code is then~~ which transmits the transaction code ~~transmitted back~~ to the host computer. Positive identification is achieved when the host computer determined transaction code matches the transaction code entered by the user. In addition, the system can ~~could~~ employ a secure user code entry interface ~~which would allow secure~~ for inputting ~~of~~ the user code.

In making the amendments set forth above, Applicant has taken care not to add new matter.

AMENDMENTS TO THE DRAWINGS begin on page 9 of this paper and include both an attached replacement sheet and an annotated sheet showing changes.

Amendments to the Claims are reflected in the listing of claims which begins on page 15 of this paper.

Remarks/Arguments begin on page 19 of this paper.

AMENDMENTS TO THE SPECIFICATION

Please amend Paragraphs [0080] through [0083] as follows:

[0080] Additional features of the dual channel schema are that the customer will be able to choose alternative user-friendly methods of identifying the TAC from the pseudo-random ~~ramndom~~ security string. such as an Enigma interface or voice recognition system. An Enigma Interface would include minor modifications to a Security Identification Module ("SIM") card in a phone or pager during manufacture but customers could avoid any calculation of the TAC themselves. Users will be able to key in their PIN and by pressing an additional key of their choice, the phone or pager will automatically compute the resultant TAC, without the customer even seeing the Security String. This computation would be a completely internal, ensuring that only the TAC is displayed, and the PIN is not retained in the mobile phone or pager. A voice recognition interface could be implemented in voice activated phones and be able to compute the appropriate TAC on the simple command "TAC!" from an approved voice.

[0081] Customers could also have the option of choosing, when applying for an enabled card, a geometric shape, as will be discussed in more detail below, in which the security string will always be delivered. The customer would simply register their chosen geometric shape to be displayed on screen and then visually apply their PIN pattern to determine the corresponding resultant TAC. This display can be interfaced by a Wireless Access Protocol ("WAP") enabled mobile phone, a third generation ("G3") mobile phone, an Internet site display prompt or a secondary dedicated terminal placed at the point of sale.

[0082] The protocol of the present invention may be `bolted-on` to an existing database server and can at least run on unmodified Electronic Funds Transfer or Point of Sale ("EFT/POS") hardware such as: (1) American Express ("AMEX"); (2) Split dial Electronic Point of Sale ("EPOS"); and (3) VISA Address Verification System ("AVS3"). In addition, the dual channel protocol can be used to upgrade the security of Mondex systems (these already use a 4-PIN digit at POS).

[0083] The dual demand schema may use a standard second generation ("G2") mobile phone, a G3 mobile phone, ~~and~~ or WAP device to receive the security string. If these devices include a modified SIM card interface for this security string the device may also include a graphical user

interface ("GUI") or an Enigma interface to simplify the derivation of the TAC.

Please amend Paragraphs [0085] through [0089] as follows:

[0085] In the direct dial scenario, the user 201 receives a security string 210 from the Authorization Server 207 which resides on the device 202. The security string 210 resides on the device 202, such as a mobile phone, until the user is ready to make a purchase. When the user 201 is ready to make a purchase they hand over, in step 220, their enabled credit card 204 to a merchant 205 to conduct the electronic funds transfer or point of sale (EFT/POS). The card 204 is swiped as usual at the merchant's 205 EFT/POS terminal. The user 201 reviews the security string 210 residing on their device 202 and determines their TAC for that particular sale. The four digit TAC 230 is provided to the merchant 205 by the user 201. The user 201 may provide the TAC verbally, by entering it into the POS terminal, or by entering the number on the mobile device 202. The credit card 204, TAC 230, and transaction amount are then sent, via the direct dial network 240, to the Authorization Server 207. The Authorization Server 207 confirms with the card issuer 209 via path 258 that the account has sufficient funds in the account and that the TAC corelates with the user's PIN number and the issued security string 210. In the event that the account number, transaction amount, and TAC are verified the Authorization Server 207 allows the transaction to proceed.

[0086] In the second scenario, referred to as the merchant acquirer network scenario, the same initial steps apply. The user 201 receives a security string 210 which resides on the device 202, such as a mobile phone, and that when the user 201 is ready to purchase an item from the merchant 205 they, in step 220, present the merchant 205 with the registered credit or debit card 204. The card 204 is swiped at the EFT/POS terminal and again the user 201 determines their four digit TAC 230, via the security string 210 residing on their mobile phone or device 202. In this scenario, the transaction information including the account number of the card ~~200~~ 204 and amount of purchase are routed via path 250 to scheme 252. The standard credit card transaction details and the pre-authorized PIN are sent to the card issuing host server 209. The scheme 252 sends the card 204 information and pre-authorization PIN to the card issuer host 209 via communications path 256. ~~At the same time, the scheme 252 communicates~~ Path 224 allows the scheme 252 to communicate with the Authorization Server 207 and verify ~~verifies~~ that the pre-authorized PIN correlates to the user's PIN. The card issuer 209 proceeds with the transaction and upon verification allows the transaction to proceed.

[0087] In addition to the dual channel schema described above, the present invention also allows for a single channel schema whereby a user would be able to use the present invention for such transactions as online purchasing via internet websites. The single channel schema and protocol is conducted via either a computer, a Wireless Access Protocol ("WAP") device, Smart Card, Proprietary System or a third generation ("G3") mobile phone, where the security string is received and the TAC transmitted on the same device. This protocol does not require a secondary channel to conduct a secure transaction.

[0088] The single channel protocol runs via an applet downloaded by the user onto their computer, WAP device or G3 mobile phone. The security string and the TAC can only be received by an enabled server and transmitted via ~~an~~ a secure sockets layer ("SSL") link. The present invention is resistant to `ghost` sites, where the user is unaware that the site they are dealing with is not certified, because the merchant (whether certified or not) would only be in possession of the users `User name or card ID` and not the relevant TAC.

[0089] The single channel solution solves the problem encountered by transmitting the relevant TAC and security string over the Internet by instructing the user's ~~users ISP (~~Web browser~~)~~ to transmit only the user name to the merchant and the relevant TAC to the enabled server/database.

Please amend Paragraph [0092] as follows:

[0092] FIG. 4 displays the main components for a preferred embodiment of the single channel schema of the present invention. The user 401 would visit the server 407 of the present invention and the server 407 would provide applets 470 for downloading to the user's device 403 via path 420. The user 401 downloads an applet 470 via path 421 which is then stored on the device 403 as the customer applet 422. The web merchant 405 would also visit the Authorization Server 475 ~~407~~ via path 450 and download ~~the~~ an applet 470 via path 451 which is stored on the merchant site 405 as merchant applet 452. The user 401 using the device 403 visits the web merchant site 405 via path 430 and selects items they wish to purchase by placing them in the basket 406 and selecting the appropriate credit or debit card for use 407. The merchant site 405 then accumulates the items in the basket 406, information about the card 407, and utilizing the merchant applet 452 routes the information along path 431 to the Authorization Server 407.

Please amend Paragraph [0102] as follows:

[0102] FIG. 8 represents an additional schema utilizing features of the present invention in which a user has a pre-authorized or debit account 804. The user would see a live device 805, such as a vending machine, and would select items via path 820 ~~810~~ thereby triggering the live device 805 to demand payment via path 810. The payment demand would be routed through the preauthorized liquid account 804 which is done by swiping the pre-authorized account 804, such as a credit or debit card, in step 840 through a card swipe device 806. In addition the micro payment demand would also notify the card swipe device 806 that a TAC would be requested. The user may have a personal device 803, such as a wireless phone, which would contain either a TAC or security string whereby the user would determine the TAC and enter the TAC 830 into the card swipe device 806. Alternatively, the user could enter the TAC 830 into the wireless device 803 which would wirelessly transmit the TAC 830 to the card swipe device 806 or Authorization Server 807. The details of the transaction are sent along path 850 from the card swipe device 806 to the Authorization Server 807. The Authorization Server 807 contains the information on the liquid account and if verified would notify a micro payment host 808 along path 860 to authorize payment. The micro payment host 808 then transfers payment along path 870 to the live device 805.

Please amend Paragraph [0117] as follows:

[0117] The inputting of a Username, Password or PIN number in a computer, portable digital assistant ("PDA"), 2.5G or 3G mobile device is currently flawed for the following reasons: (1) the User can be seen from onlookers entering their PIN number into the device (called `shoulder surfing`); (2) the keyboard could contain a `Trojan` program that records the inputted Username, Password or PIN number (Trojans are downloaded without the knowledge of the User onto a computer and can reside there indefinitely); (3) PKI Certificates authenticate that the transaction was conducted on a certified computer, but they do not effectively authenticate the User behind the computer; and (4) computers running Microsoft Windows have a problem because Windows remembers the Username, Password or PIN number which creates a situation where the device stores the I/D of the User within the computer.

Please amend Paragraph [0121] as follows:

[0121] Further, the user interface is easy to use because the user need know nothing about the protocol, TAC's and Security Strings. The PIN Safe user would merely input their unchanging PIN via the Pin Safe user interface. Further, the Pin Safe user interface is "tempest" proof because the interface does not display the users PIN or TAC (Pseudo PIN) on screen, and therefore is not subject to Electro-magnetic emissions from the video display unit ("VDU") that could be the subject of surveillance via Tempest technologies. The strong protection gained by using the Pin Safe user interface of the present invention allows safe single PIN usage on a variety of accounts with differing security architectures which can be achieved by using a central PIN Authorization Server. Even if the security string resides on the device it is not a problem because the present invention does not require a digital certificate and therefore there is nothing in the memory of the computer that compromises the Users I/D if it falls into the wrong hands.

Please amend Paragraph [0130] as follows:

[0130] In addition, the Pin Safe or Radar Interface can work within a computers own processor, within a local area network ("LAN") configuration, and over the Internet. Operating within a computers own processor the Pin Safe interface could act as a hack proof screensaver which means that when a user first started their computer they will be presented with the interface. The user must input their PIN accordingly and if the user decided to leave the computer for a short time, where there is the opportunity for criminal use of his computer, the user could press a function key which would activate the Pin Safe interface. Upon returning to the their computer they would simply click on their mouse or any key and enter their PIN via the Pin Safe interface.

Please amend Paragraph [0137] as follows:

[0137] As seen in FIG. 18, the Security String is sent from authorization computer 1807 to the User's mobile device 1804. The user 1801 inputs the TAC via the Pin Safe interface 1823 and the Authorization Server 1807 receives the TAC via the Internet 1813.

Please amend Paragraphs [0141] and [0142] as follows:

[0141] FIG. 21, shows a typical data access application where an Authorization Server 2107 has

been fitted to a Gateway Server 2109 accessing a Database 2111, the Database 2111 being protected by a firewall 2115. FIG. 21 assumes that the user 2101 has registered with the system and has the Pin Safe Interface applet 2123 on their computer which allows the user 2101 to communicate with Authorization Server 2107 via the Internet 2113 using paths 2120, 2140, and 2152. To access information from the Database 2111 the Authorization Server 2107 sends a new security string to the user's computer or G2 mobile phone 2104 via the Internet 2113 or through a wireless connection 2151. The security string 2151 resides on the device 2104 until the user 2101 wishes to access the Database 2111.

[0142] The User 2101 sends his volatile TAC to the Authorization Server 2107 to confirm his/her identity. In the dual channel scenario the user obtains their TAC from the G2 mobile device 2104 via either visual extraction (using their PIN as a sequencer) or Smart PIN or standard inline memory module ("SIMM") extraction where the User 2101 enters their PIN into the device 2104 and the relevant TAC digits are displayed on the device 2104 screen. The TAC is then inputted into the user's computer (not shown). In the single channel scenario the user simply inputs their PIN into the Pin Safe interface 2123. The PIN is then converted into a TAC within the applet 2123 and transmitted via path 2120 to the Authorization Server 2107

Please amend Paragraph [0146] as follows:

[0146] FIG. 23 shows the Generic Integration Platform which displays the Authorization Server 2307 inside a firewall 2315~~-2215~~. The Authorization Server 2307 is connected to a Net Server 2317 and a host database 2311. The host database 2311 may also be inside it's own firewall 2316.

Please amend Paragraph [0148] as follows:

[0148] Any reference herein to a computer means any personal computer, ATM, PDA, G2.5 Mobile Device, G3 Mobile Device, or any device with a central processing unit ("CPU"). Any reference herein to a transaction means any financial transaction, remote Data Access procedure, or any interface transaction between a user and a system. The numbers on the various user interfaces and displays are merely exemplary and the use of characters, letters, colors and such may be used individually or in combination and still fall within the intended scope of the present invention.

Please amend the Abstract as follows:

A method and system for secure identification of a person in an electronic communications environment, wherein a host computer ~~is adapted to be able to~~ communicates with a plurality of user-operated electronic devices. ~~operated by the user. The user is issued with a user code, known only to the user and stored in the host computer.~~ When the user is required to identify themselves to the host computer, the host computer generates a pseudo-random security string and applies a previously issued ~~the~~ user code to the ~~pseudo-random~~ security string to generate a transaction code. The host computer also transmits the ~~pseudo-random~~ security string to one of the electronic devices for display ~~which is displayed by the electronic device~~ to the user. The user applies the ~~their known~~ user code to the displayed ~~pseudo-random~~ security string and determines the transaction code. The ~~user enters the~~ transaction code is entered into an electronic device ~~and the entered transaction code is then~~ which transmits the transaction code ~~transmitted back~~ to the host computer. Positive identification is achieved when the host computer determined transaction code matches the transaction code entered by the user. In addition, the system can ~~could~~ employ a secure user code entry interface ~~which would allow secure~~ for inputting ~~of~~ the user code.

In making the amendments set forth above, Applicant has taken care not to add new matter.